UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/625,547	07/25/2000	Laurence Hamid	12-52 US	7157

7590 05/20/2005

Gordon Freedman
Freedman & Associates
117 Centrepointe Drive
Suite 350
Nepean, ON K2G 5X3
CANADA

EXAMINER	
ZAND, KAMBIZ	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 05/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/625,547	HAMID ET AL.	
	Examiner	Art Unit	
	Kambiz Zand	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 December 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *1-8* is/are allowed.

6)☒ Claim(s) *9-13 and 15-20* is/are rejected.

7)☒ Claim(s) *14* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12/14/2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The text of those sections of Title 35,U.S.Code not included in this section can be found in the prior office action.
2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
3. Claims 1-20 have been amended.
4. Claims 1-20 are pending.
5. Examiner withdraws objection to the drawings and specification due to correction by the applicant.
6. Examiner withdraws rejection of claims under 35 U.S.C 112-second paragraphs due to correction by the applicant.

Response to Arguments

7. Applicant's arguments filed 12/30/2004 have been fully considered but they are not persuasive with respect to claims 9-13 and 15-20.

- In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e. " modifying password"; "master password","changing the secure file to be accessible with the master password absent accessing the database of passwords") are not recited in the rejected claim(s). Although the claims are

interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Examiner however considers Nelson's second password that accesses the password database as corresponding to Applicant's second password. The passwords in the database do safe guard the files since by choosing those password one can access the files.

Claim Rejections - 35 USC § 103

8. **Claims 9-10** are rejected under 35 U.S.C. 103(a) as being unpatentable over He (5,944,824 A) in view of Brown et al (6,618,806 B1).

As per claim 9 He (5,944,824 A) teach a method of providing improved security for files accessible by password data entry **(see col.2, lines 25-28 where a method of accessibility of a system using password that addresses the security of the system is disclosed)** comprising the steps of: selecting a secured data file **(see col.1, lines 23-30 where NEs are described as switches, databases and other network resources. Examiner considers other network resources corresponds to Applicant's secure data file since secure data file is a resource; fig.12, item 312-322 disclose the process of returning the list of NEs or secure files, item 324**

disclose selection of the user from the list and therefore selecting the NE user request access as depicted in item 326); providing a password database **(see col.10, lines 37-40 disclose database of 13 is located within the security server 15; col.9, lines 29-31 disclose passwords are stored in the security server database where the database 13 corresponds to password database of Applicant; col.10, lines 42-54 disclose the records of user accounts store in the database 13 contains field such as present password or new password)**; when the individual is authorized **(see fig.5, item 104 where user is authenticated)**, retrieving the secure password from the database **(see fig.4, item 92 where retrieve user's password for accessing reasons are being done by recovery procedure that could be manual or automatic)** and automatically providing the secure password to the selected secured file password entry subsystem **(see fig.4, item 79, 84, 88 and 98; col.8, lines 9-15 disclose determining a secure password for entry subsystem NEs and item 79, 84 and 86, 96 where the password generation and recovery or retrieving may be automatic and secure since it is protected)**; automatically determining a secure password identifier associated with the secured data file **(see item 312 of fig.12 where passwords corresponding to NEs or secure files and user accounts are created; col.14, lines 44-47 disclose the log-on procedure is automatic and therefore such association is determined automatically)** but do not explicitly determining a user authorization method having an associated security level sufficient for accessing the secure password; authorizing an individual according to the secure authorization method. However Brown et al (6,618,806 B1) teach determining a user authorization method

having an associated security level sufficient for accessing the secure password; authorizing an individual according to the secure authorization method **(see col.5, lines 5-29 where based on different set of instructions that corresponds to Applicant's associated security level a different biometric challenge being conducted that corresponds to Applicant's different methods and if verified the secure password is being retrieved for access)**; authorizing an individual according to the secure authorization method **(see col.5, lines 5-29 where based on the verification of biometric challenge authorization is being done by verification; col.8, lines 37-65 details the different authorization method or authentication)**. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Brown's biometric authorization methods that corresponds to different rules based on different instructions where the biometric information's are stored in the database in He's single sign-on NEs databases method of access authentication in order to provide an authentication rule associated with a user based on different parameters of biometric data of a user.

As per claim 10 He (5,944,824 A) teach the method of providing improved security for files accessible by password data entry as defined in claim 9 wherein the password database comprises a plurality of passwords **(see col.9, lines 29-30 disclose database stores passwords that corresponds to a plurality of password and col.4, lines 14-18 where it disclose databases)** and wherein the step of determining a secure password identifier comprises the step of determining a password from the

plurality of passwords for use in accessing data within the secured data file **(see col.6, lines 13-23 disclose authorization uses an access control list for NEs entries by a user; col.5, lines 7-14 disclose based on selection of a password of a user and authentication access is being granted).**

Claim Rejections - 35 USC § 102

9. **Claims 11 and 15-19** are rejected under 35 U.S.C. 102(e) as being anticipated by Nielson (6,182,229 B1).

As per claim 11 Nielson (6,182,229 B1) teach a method of changing a first password for securing files accessible by password data entry comprising the steps of: determining a plurality of files secured with a first password **(see col.3, line67 and col.4, lines 1-2 where passwords within the database protect the remote server; col.3, lines 12-22 where a table with each entry of URL specifies the site access protocol and the name of the site where each URLs corresponds to plurality of files (please see definition of URL in a computer dictionary), and the encrypted password that corresponding to a url file as depicted in fig.2 corresponds to Applicant's first password that secure the file)** ; providing a second other password for securing the plurality of files **(see col.3, lines 21-24 disclose a master password that being used to encrypt the passwords for the remote server entry and**

possibly the ids, this master password corresponds to the second password that protects security for the urls by encrypting the access password of url); for each file secured with the first password, accessing the file with the first password **(see fig.2 where the first password corresponds the url is used to access the web site once is decrypted, it also can be done manually or automatically)** and securing the file with the second other password **(see col.3, lines 21-24 disclose a master password that being used to encrypt the passwords for the remote server entry and possibly the ids, this master password corresponds to the second password that protects security for the urls that corresponds to files that are being secured)** ; storing the second other password in the password database **(see col.4, lines 34-36 where it disclose the master password that corresponds to Applicant's second password is stored in the memory; fig.3, item 312 and 314 disclose the master password or second password stored in the password database)**.

As per claim 15 Nielson (6,182,229 B1) teach the method of changing a first password for securing files accessible by password data entry as defined in claim 11 wherein the step of determining a plurality of files secured with the first password comprises the step of determining from the password database, files associated with the first password **(see col.3, line67 and col.4, lines 1-2 where passwords within the database protect the remote server; col.3, lines 12-22 where a table with each entry of URL specifies the site access protocol and the name of the site where each URLs corresponds to plurality of secure files and the encrypted password**

corresponding to a url file as depicted in fig.2 corresponds to Applicant's first password).

As per claim 16 Nielson (6,182,229 B1) teach the method of changing a first password for securing files accessible by password data entry as defined in claim 15 wherein those files associated with the first password are identified because they are identified by an identifier associated with the first password **(see fig.2 where user id associate with their corresponding password and file url; col.3, lines 48-53 where the association with controlled web site or a page. Examiner has considered address of secure web site URL as a file that need password for access since url address could corresponds to a particular file for access).**

As per claim 17 Nielson (6,182,229 B1) teach the method of changing a first password for securing files accessible by password data entry as defined in claim 11 wherein the step of determining a plurality of files secured with the first password comprises the step of determining from accessible files, those files associated with the first password **(see fig.2 where user id associate with their corresponding password and file url; col.3, lines 48-53 where the association with controlled web site or a page. Examiner has considered address of secure web site URL as a file that need password for access since url address could corresponds to a particular file for access and they are secure since the password and possibly user IDs are encrypted as depicted in fig.2).**

As per claim 18 Nielson (6,182,229 B1) teach the method of changing a first password for securing files accessible by password data entry as defined in claim 11 wherein the step of providing a second other password includes the step of automatically generating the second other password **(see col.5, lines 555-61 where it disclose passwords can be generated automatically by password management)**.

As per claim 19 Nielson (6,182,229 B1) teach the method of changing a first password for securing files accessible by password data entry as defined in claim 18 wherein the method of changing first password is automatically repeated at intervals **(see col.19-20 where it disclose the password particular to specific site (URL address (file) could be random for enhancing the security where such password corresponds to Applicant's first password as detailed in claim 11 above)**.

10. **Claims 12, 13 and 20** are rejected under 35 U.S.C. 103(a) as being unpatentable over Nielson (6,182,229 B1) in view of Bellemore et al (6,145,086 A).

As per claim 12 Nielson (6,182,229 B1) teach all limitation of the claim but do not explicitly disclose the step of changing password includes: archiving the first password for use in accessing archival files secured with the first password. However Bellemore et al (6,145,086 A) disclose security and password mechanism with relationship to a

database where the process of changing a password includes archiving the password as old password **(see col.5, lines 23-27 where it disclose history table contains used password as also depicted in fig.5, item 209)**. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Bellemore et al's history table in Neilson's password database in order to archive old passwords for approval of new password and by comparison means to be sure the new password does not be the same as last N old passwords.

As per claim 13 Nielson (6,182,229 B1) teach all limitation of the claim but do not explicitly disclose the step of authorizing an individual requesting a change of the first password prior to changing the first password. However Bellemore et al (6,145,086 A) disclose the step of authorizing an individual requesting a change of the first password prior to changing the first password **(see col.6, lines 58-63 where the request for change of password is being done by client that corresponds to Applicant's individual)**. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Bellemore et al's history table and password change request in Neilson's password database security method in order to determine whether the proposed password may be used as a password by archive old passwords for approval of new password and by comparison means to be sure the new password does not be the same as last N old passwords .

As per claim 20 Nielson (6,182,229 B1) teach the method of changing first password is automatically repeated at intervals **(see col.19-20 where it disclose the password particular to specific site (URL address (file) could be random for enhancing the security where such password corresponds to Applicant's first password as detailed in claim 11 above)** but do not disclose explicitly changing the password is repeated upon detection of a breach of a password and upon expiry of a password. However Bellemore et al (6,145,086 A) disclose the method of automatically changing the password is repeated upon detection of a breach of a password and upon expiry of a password **(see fig.3, item 310, 314 and 318 where determination is made for breach of a password by monitoring the number of failed attempt; item 360, 370 and 328 in fig.3 represent the expiry of password monitoring)**. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Bellemore et al's history table and password change rules in Neilson's password database automatic password generation security method in order to invoke a security process in response to client transmission of a connection message to the database management.

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (571) 272-3811. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone numbers for the organization where this application or proceeding is assigned as (703) 872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kambiz Zand

05/12/2005

AU2132

Replacement page

Fig1-6 All drawings approved 05/12/05

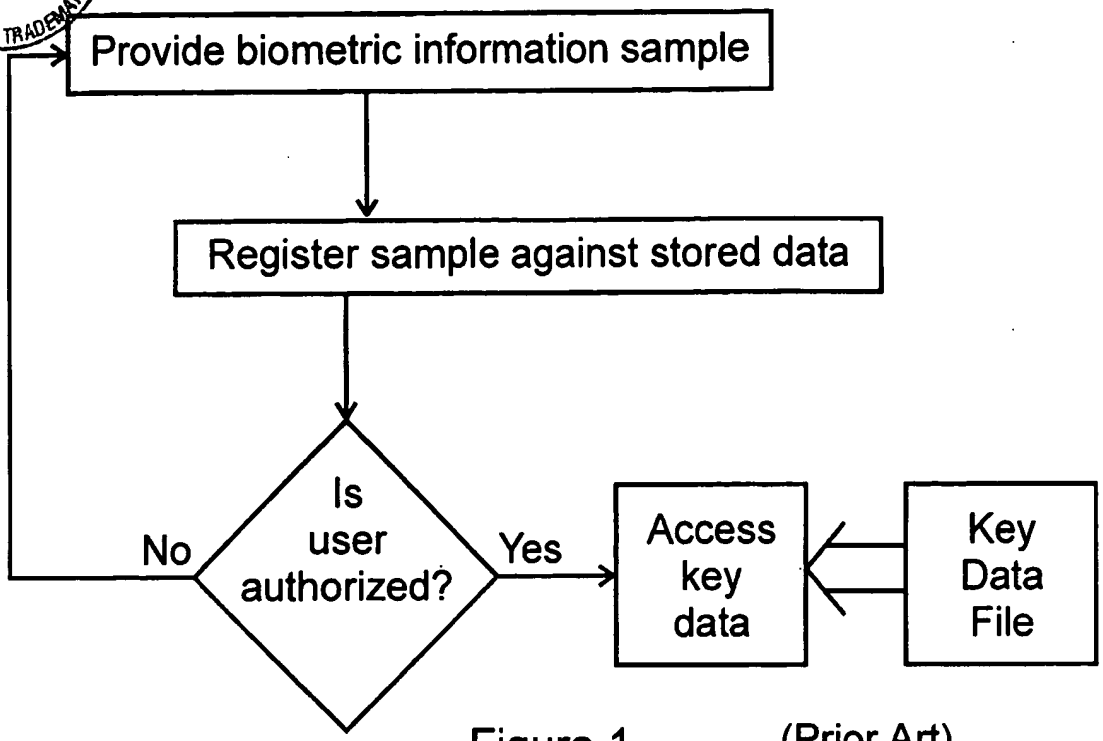

Figure 1 (Prior Art)

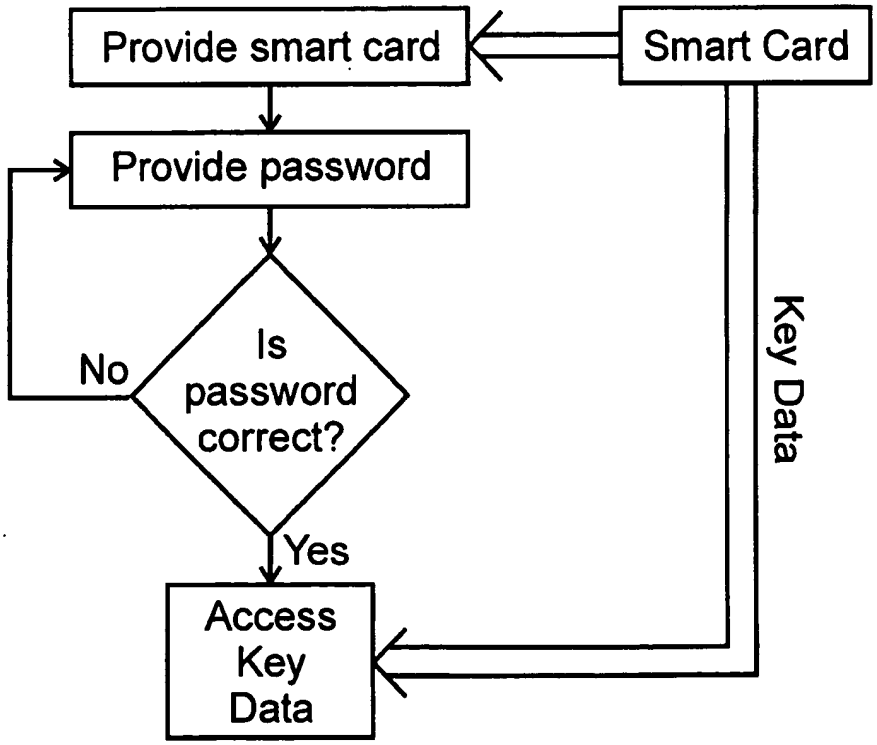

Figure 2 (Prior Art)

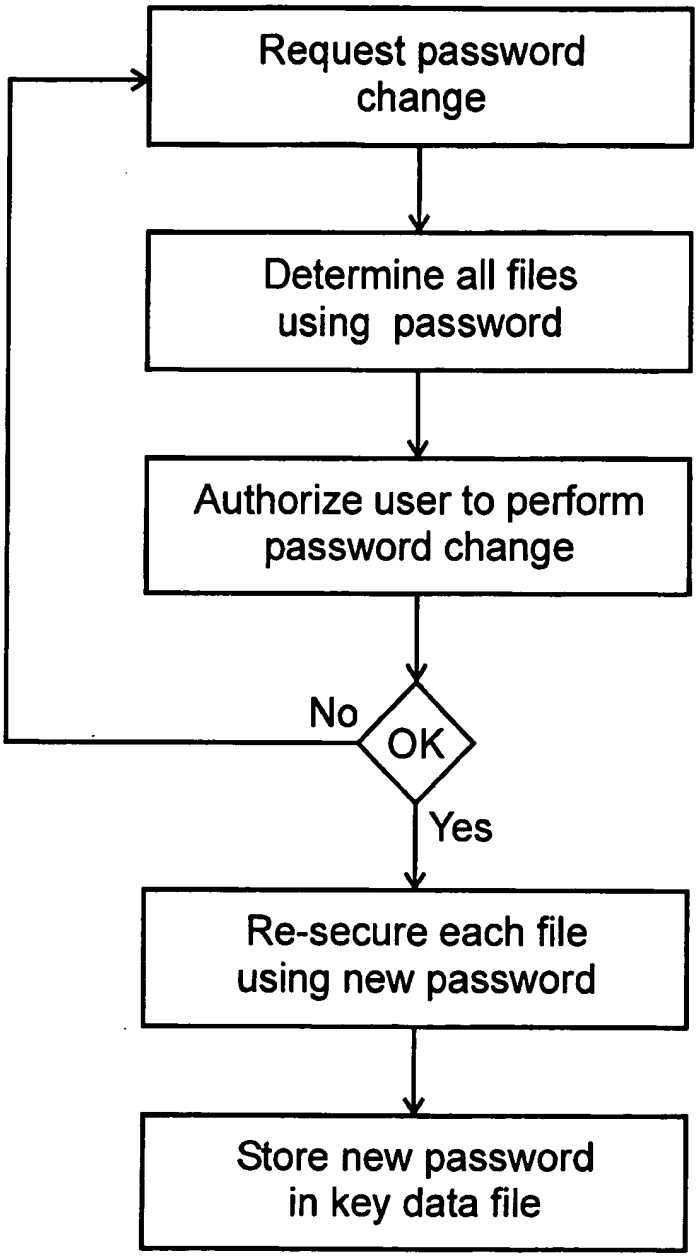
Request password change
Determine all files using password
Authorize user to perform password change
No
OK
Yes
Re-secure each file using new password
Store new password in key data file

Figure 7

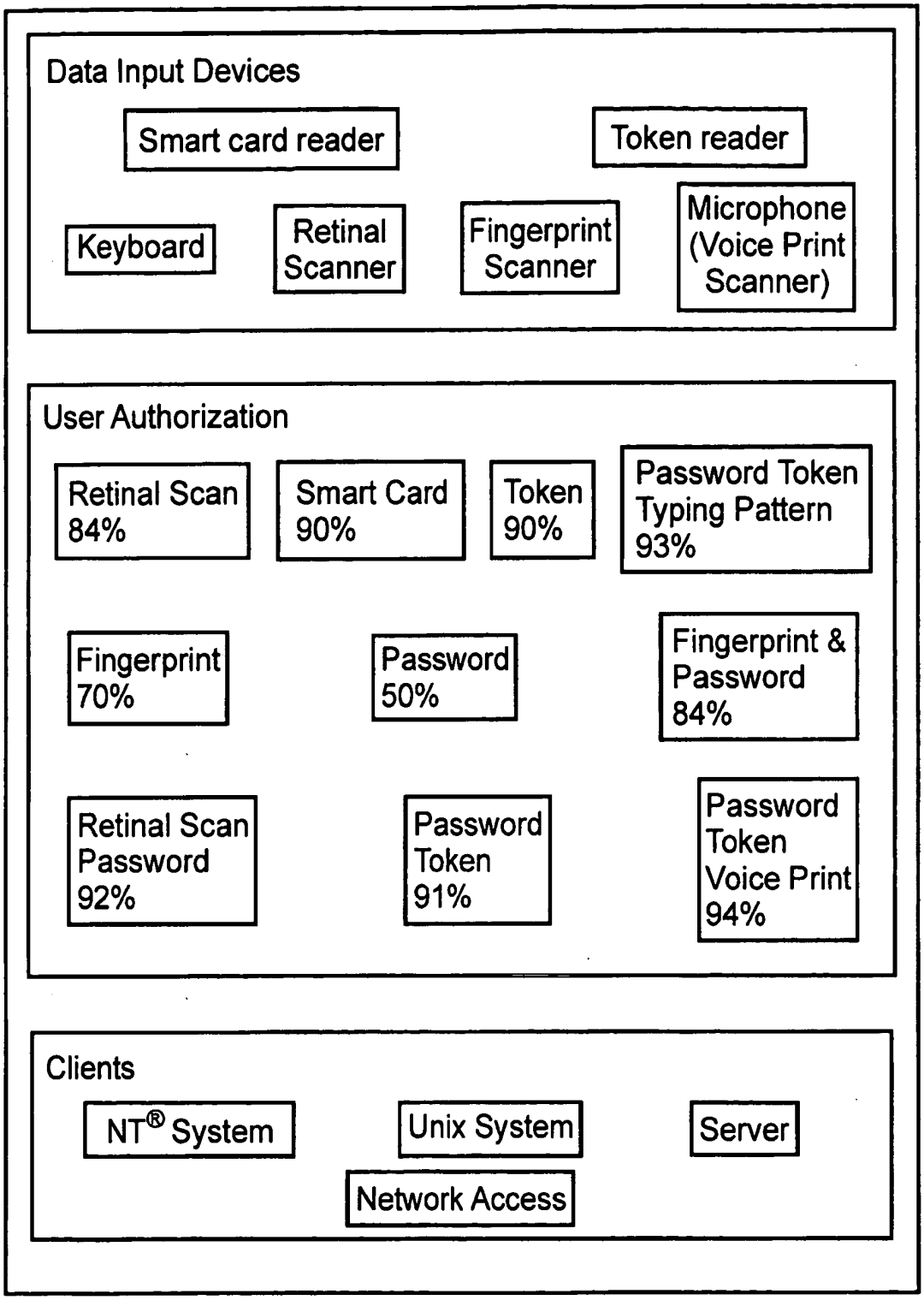
Data Input Devices
Smart card reader
Token reader
Keyboard
Retinal Scanner
Fingerprint Scanner
Microphone (Voice Print Scanner)
User Authorization
Retinal Scan 84%
Smart Card 90%
Token 90%
Password Token Typing Pattern 93%
Fingerprint 70%
Password 50%
Fingerprint & Password 84%
Retinal Scan Password 92%
Password Token 91%
Password Token Voice Print 94%
Clients
NT® System
Unix System
Server
Network Access

Figure 3

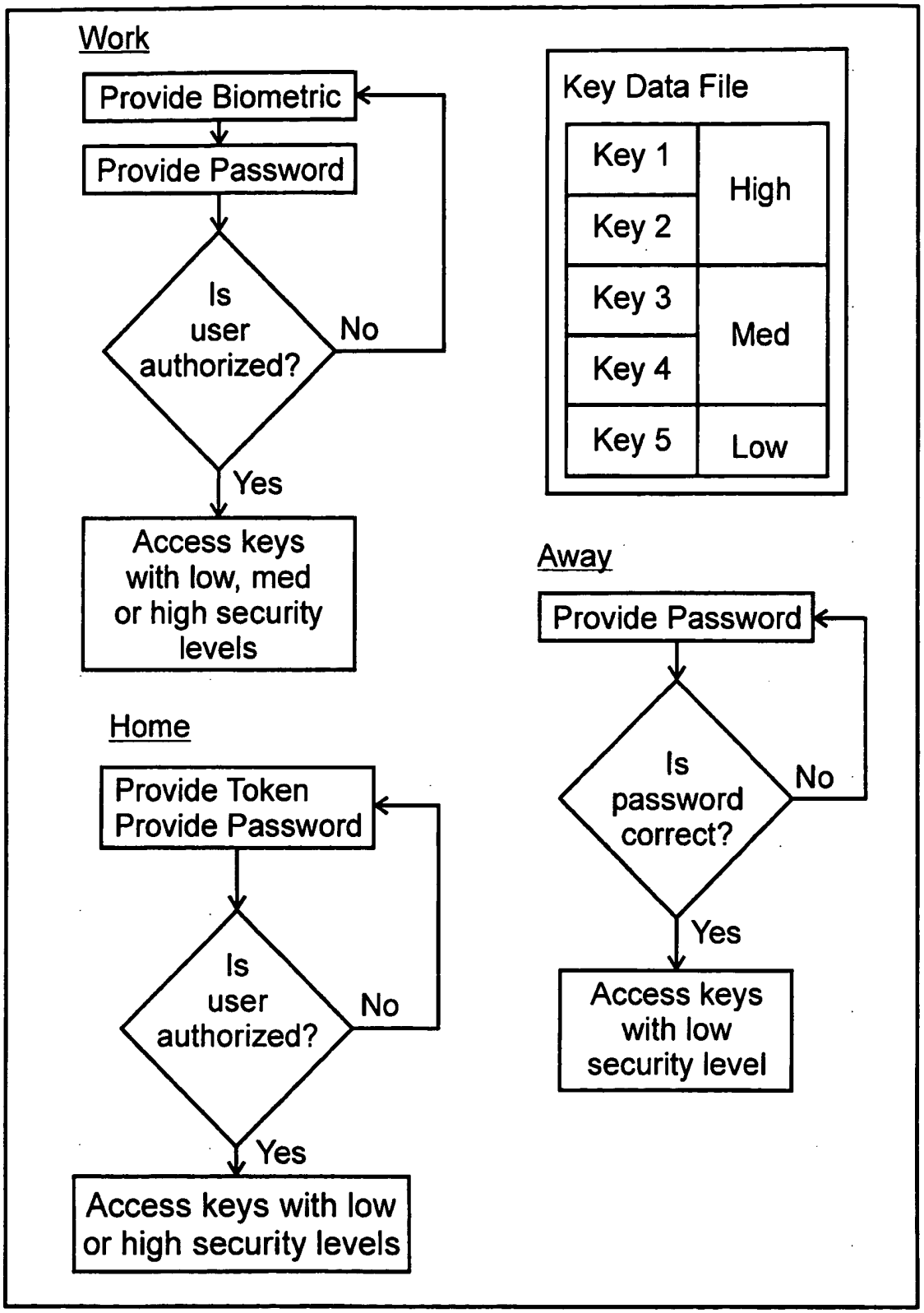
Work
Provide Biometric
Provide Password
Is user authorized?
No
Yes
Access keys with low, med or high security levels
Key Data File
Key 1
Key 2
High
Key 3
Key 4
Med
Key 5
Low
Away
Provide Password
Is password correct?
No
Yes
Access keys with low security level
Home
Provide Token
Provide Password
Is user authorized?
No
Yes
Access keys with low or high security levels

Figure 4

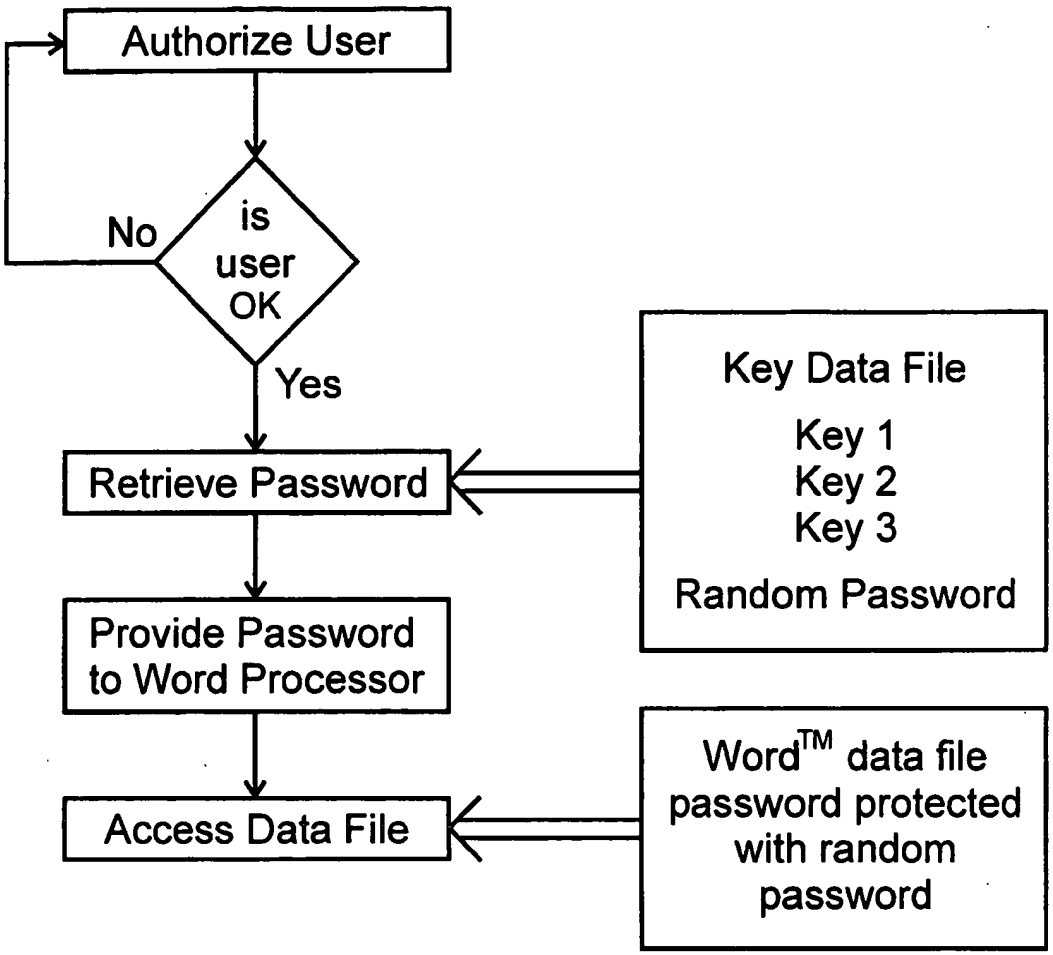
Authorize User
is user OK
No
Yes
Retrieve Password
Provide Password to Word Processor
Access Data File
Key Data File
Key 1
Key 2
Key 3
Random Password
Word™ data file password protected with random password

Figure 5

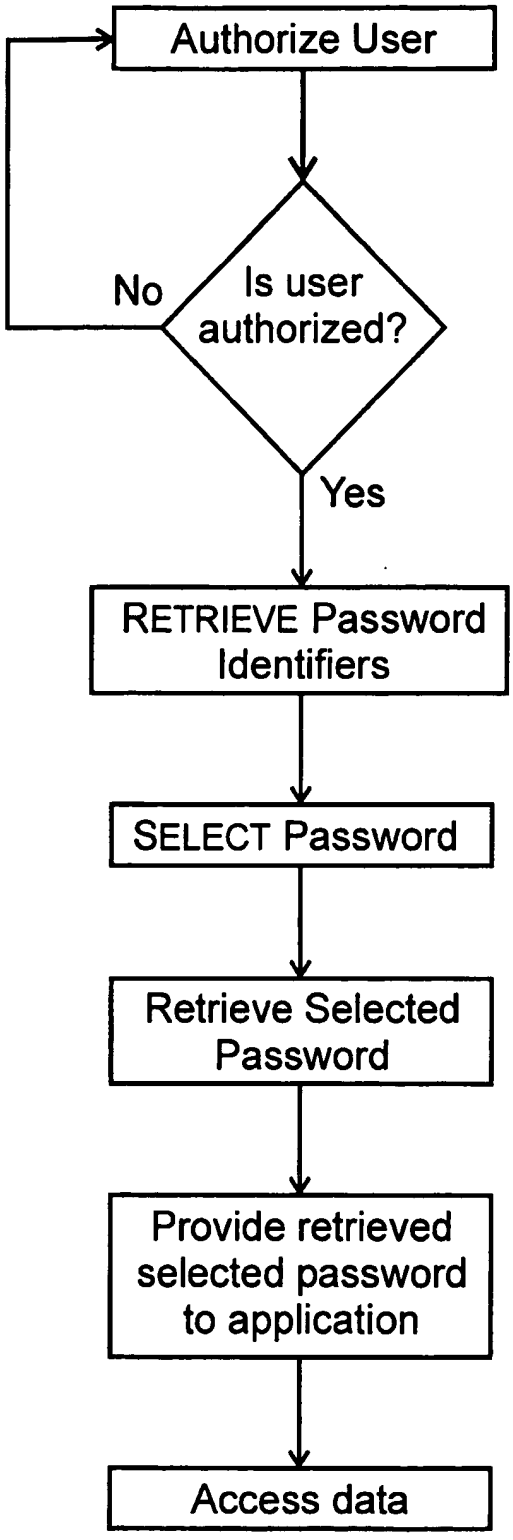
Authorize User
Is user authorized?
No
Yes
RETRIEVE Password Identifiers
SELECT Password
Retrieve Selected Password
Provide retrieved selected password to application
Access data

Figure 6